PROJEKT

Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia

Previazané s balíkom KPB6 – Publikačné výstupy

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

ÚRAD VLÁDY
SLOVENSKEJ REPUBLIKY

Trends, enterprise network design and the use of AI

Pavel Segeč
Department of Information Networks
Faculty of Management Science and Informatics
Žilina, Slovakia
pavel.segec@fri.uniza.sk

Patrik Grexa
Department of Information Networks
Faculty of Management Science and Informatics
Žilina, Slovakia
grexa@stud.uniza.sk

Jozef Papán
Department of Information Networks
Faculty of Management Science and Informatics
Žilina, Slovakia
pavel.segec@fri.uniza.sk

Jana Uramová
Department of Information Networks
Faculty of Management Science and Informatics
Žilina, Slovakia
pavel.segec@fri.uniza.sk

***Abstract*— This paper examines the changing dynamics of enterprise networking with particular attention to design, trends, and impact of AI on network operations. We are trying to provide an insight into the multilayered enterprise network design and its benefits for scalability, security, and integration with modern technologies such as SD-WAN, virtualization, and SDN. The paper continues with wired LAN and wireless LAN architectural design considerations, focusing on cloud integration for improved security and manageability. We describe how SD-WAN, SASE, and SSE fit in network modernization and management security. A large volume of this paper is devoted to current developments in enterprise networks, including decentralized network management, security operations via AI-powered tools, and evolutions in intelligent monitoring made possible by machine learning and AI. To conclude, the study presents five AI assistants (ChatGPT, Standard Copilot, Google Gemini, Grok, and DeepSeek) that generate Cisco switch configurations and analyze CLI show outputs. Our results show various capabilities of these AI models, further improving and stimulating their potential to assist in high level network engineering tasks toward making network operations more automated and efficient.**

Keywords—Network Operative, AI Assistants, Enterprise Network, Cisco

I. Introduction

Enterprise networks form the backbone of today's organizations. They facilitate the secure and efficient transmission and management of information within and outside. The designed capacity for very high data security and integrity has proved to be an evolutionary factor in the architecture of enterprise networks. Enterprise networks gradually moved toward a multi layered model of access, distribution, and core. This shift in architecture enables the network to scale well and be clear and available, while also allowing seamless integration with cloud and software defined solutions. With digital transformation being accelerated and network infrastructures being more complex than ever, design principles have to be reconsidered, and fresh concepts have to be embraced.

From foundational built network design to Wireless Local Area Network and Wired Local Area Network architectures, this paper goes into realms that include Software Defined Wide Area Networking (SD-WAN) and Secure Access Service Edge (SASE). They provide solutions for increased security level and a directly managed service setup at locations that are physically apart. We are then talking about the utmost advantage from Artificial Intelligence and Machine Learning technologies. Namely, AI-assisted auto-remediation, anomaly detection and predictive analysis that are converting network management, monitoring, and security significantly. Trends such as decentralization of network management, convergence of security disciplines and rise of intelligent correlation monitors will occur. We are exploring the top-rated AI assistants and testing their competence in fulfilling core network engineering tasks, such as switch configuration generation and CLI output interpretation. Doing so gives us insight into their present capabilities and potential to change network administration in the near future.

II. Enterprise Network Design

Enterprise networks can provide corporations with the transmission and management of information both within institutions and between them. Since both companies and individuals place great importance on ensuring that unauthorized parties do not gain access to their data, organizations focus on achieving the highest possible levels of data transmission security and integrity. These efforts are also reflected in the design of enterprise networks.

Enterprise network design is the process of planning, designing and implementing an IP network with the goal of ensuring high reliability, security, speed, as well as easy scalability and manageability [1]. In the past, enterprise networks were structured with a focus on centralization. Today, we observe the use of a multi-layered model, which can be divided into several layers: access, distribution, and core [3]. The multi-layered model allows the network to be segmented into different parts, enabling simple scalability, clarity, and improved network availability. Since, in the event of device failure, another device can take over its role. It also supports the integration of cloud and software-based solutions by providing a structured network for connecting users and devices to these services. This architecture enables efficient cloud access, traffic management, and integration with technologies like SD-WAN, virtualization, and software-defined networking (SDN). These technologies are

becoming an essential part of modern enterprise networks [1], [2].

A. Wired and Wireless LAN

Wired and Wireless LAN architectural design must accommodate a variety of deployment scenarios beginning with a single device at a small site to large infrastructures spanning multiple buildings with several wired and wireless connectivity requirements. Some deployments require greater degrees of availability and minimum risk tolerance, and others conduct a reactive fix-on-failure option that can tolerate temporary service interruptions. Platform selection, vendor usage, and device capabilities are considered. A setup, which often contains separate access and distribution layers, makes it challenging to aggregate access switches. Although somewhat flexible to meet Layer 2 adjacency requirements across multiple wiring closets, it brings about problems with configuration and protocol management. An alternatives could be made to utilize stacking at both the access and distribution layers. An alternative extends Layer 3 connectivity all the way up to the access layer, promising higher consistency, scalability, and availability than a multilayer design. This is chiefly realized through campus fabric technologies, taking care of the network administration automatically and optimally. Wireless integration generally overlays, relying upon the wired infrastructure placed underneath. In the realm of large-scale networks, dedicated devices work to bolster capacity while smaller deployments may be streamlined and optimized [3].

1) Cloud integration

Cloud networks became an increasingly favorable option for companies due to the possibility of improved security, availability and improved monitoring. Centralized control and monitoring of network devices may be achieved using a cloud platform, eradicating the need to maintain complex hardware infrastructure. Companies demand better availability and security for some devices, which benefits administrators by simplifying daily mundane tasks and offering a single view of the whole network infrastructure. Integration with existing identity and security services hosted on-premises or in the cloud, such as RADIUS and Active Directory, allows consistent enforcement of policies and user authentication on the network. One crucial aspect is an integrated wired and wireless network under a single cloud management framework. Using centralized management interfaces hosted on a cloud platform is the backbone of cloud management network designs that allow efficient configuration, monitoring, and enforcement of policies. Secure connectivity through strongly encrypted APIs and robust authentication mechanisms goes a long way to ensure that data is protected and restricted from unauthorized access. Cloud networks are scaled to high availability by using hierarchical topologies and dynamic routing protocols. Continuing performance testing, monitoring, and validating maintains reliability and keeps cloud integration optimized [10].

B. SD-WAN

SD-WAN solution is a modern approach of managing and operating a wide-area network. Typically, the solution accounts for a central management platform that makes it easy to configure, set policies for, and monitor the network devices on geographically dispersed locations. One of the features of this solution is application aware routing that selects, in real time, the best path for network traffic flow according to the needs of the application and the characteristics of the available WAN transports. When integrating SD-WAN, it is important to enforce strong security mechanisms, including end-to-end encryption and network segmentation, to guarantee data protection and traffic separation. Giving branches direct access to the internet would enhance performance by cutting latency caused by backhauling internet bound traffic from a branch to a central data center. Setting up a network for SD-WAN integration requires setting up the central control and management components such that they are highly available. This is often done with cloud infrastructure or on-premises infrastructures that are geographically redundant. Edge devices in branch offices and data centers should be able to connect to multiple WAN transports at the same time to harness resilience and bandwidth. Automating on a large scale, including zero-touch provisioning, is pertinent to the smooth deployment and management of edge devices; consequently, the SD-WAN fabric could also be extended to cloud so that consistent performance and policies are applied to cloud-hosted applications [1], [4].

C. SASE/SSE

SASE is described as the contraction of networking (SD-WAN) and Security Service Edge (SSE) functions meant to be provided from the cloud, melding the strengths of these two functions and solving problems inherent in the traditional data center-based approaches to networking. SSE incorporates cloud-delivered security services primarily consisting of DNS-layer security, Secure Web Gateway (SWG), Firewall-as-a-Service (FWaaS), Cloud Access Security Broker (CASB), and Zero Trust Network Access (ZTNA). It focuses on describing the secure, seamless access of applications from any location, on any device, with strict consideration of identity, context, and least privilege access. Digital Experience Monitoring (DEM) is also highlighted for providing end-to-end visibility. Good practices when deploying SASE and SSE include maintaining a cloud-first security architecture that merges formerly disparate security functions into one cloud-delivered service. Follow Zero Trust principles to treat every access attempt with verification of identity, context, and least privilege access to applications. Use Digital Experience Monitoring for end-to-end visibility to measure user and application performance across different network paths and to resolve issues proactively. While designing the network, the focus is on enabling transition from data centric to cloud enabled architecture where security enforcement points are closer to users and applications wherever they may reside. This implies routing traffic to cloud security services (SSE) for inspection and policy enforcement. Integrate SD-WAN for optimized and secure connectivity to cloud applications and to the internet [5], [1].

III. Current Trends and AI Operations in Enterprise Networks

Significant leadership shifts mark this evolution of enterprise networks, in whose disciplines there are changes

in management, security, monitoring, and the rise of AI. Distributed and autonomous approaches are gradually taking central-stage away from traditional centralized management, driven by virtualization, software-defined networking, and complexity in distributed systems. Security involves employing collaborative approaches, integrating technologies, and implementing principles of Zero Trust. Network monitoring is becoming proactive and intelligent, utilizing AI and machine learning for sophisticated detection of threats and adaptation to zero trust. Lastly, AI operations development is impacting network infrastructure optimally for automation, anomaly detection, securing, and enhancement, promising to pave the way for intelligent, self-managing networks.

1) Centralized network management

Rapid virtualizing of network infrastructure and the increased acceptance of software-defined networking require a management paradigm to dynamically adapt to or orchestrate abstracted resources. Networks are increasingly needing to be agile and flexible to support changing business requirements, thus rendering static, centralized models quite ineffective. The evolution of geographically distributed systems from cloud computing to edge computing introduces a level of complexity that offers challenges to purely centralized control. Therefore, modern networks, considered as interconnected "systems of systems," need to be equipped with management that ensures smooth interoperability across multiple technologies. The scalable nature and complexity of modern day telecom networks expose inherent limitations, such as a single point of failures, the bottleneck in scalability, latency increase in a distributed environment, and security dangers emanating from a central point of attack. Thus, the trend in network management points towards decentralized and autonomous methodologies aiming at improving the resilience, scalability, and responsiveness of networks by distributing control and employing smart automation. Accordingly, DePIN (decentralized physical infrastructure networks), decentralized AI, and decentralized cloud computing are expected to significantly contribute to future network management alongside enhancements in network automation, orchestration, AI, and machine learning to transform network management. This level of evolution is designed to provide stronger, more sensitive, and secure network infrastructures that can fulfill the requirements of the expanding digital world [2].

2) Security Convergence

The emergence of Cyber Physical Systems and growing dependence on IoT devices renders the implementation of a unified security platform necessary, whereby opportunities will be observed and secured, digital and physical alike. An integrated security system provides a "single pane of glass" view of risk; therefore, threats are detected and responded to in a concerted way. The importance of cloud-based solutions in the convergence of security operations is laid in the domains of scalability, adaptability, and real-time update mechanisms. AI is yet another probable big contributor in the convergence of security. AI-based tools pinpoint the threat by working through huge datasets registering abnormal behavior that could indicate intrusion or malicious activity either cyber or physical. They also serve in automated responses to threats, so incidents can be swiftly mitigated. The proposed integration of AI into SIEM systems further builds up the ability to correlate events and generate comprehensive security insights. In conclusion, the convergence of network security has become a paradigm shift that implies the new face of integrated and more forefront security. By synergizing disparate security domains, enacting technological means like AI, and applying principles like Zero Trust, organizations shall form robust security matrices that are comprehensive and highly interwoven against a rapidly changing threat landscape [7].

3) Monitoring

The present scenarios of network monitoring give birth to the paradigm shift directed at proactive and intelligent monitoring strategies precipitated by the increasing complexities and security concerns brought about by modern network architectures. The integration of advanced analytical techniques, of which machine learning and artificial intelligence constitute major categories, is a prominent and growing trend, improvising threat detection and response mechanisms. These detection and response processes move beyond traditional signature detection systems and are thus able to accurately and swiftly spot behavior that departs from the norm in networks and potential security violations. In addition, the establishment of zero-trust security models is profoundly altering methods of network monitoring. In this paradigm, verification is always upheld with regard to every user and device seeking to gain access to network resources, factoring in real-time monitoring of access patterns and user activities related to any network layer as requirements. At this juncture, monitoring systems are accordingly being enhanced with a view to incorporating such mechanisms as highly granular visibility and strong contextual awareness to enable enforcement of stringent access control and identification of lateral threats. The other major trend concerns heightened emphasis on securing the network access layer under consideration. Research points to numerous weaknesses at this level, encouraging the deployment of specialized security protection systems. Typically, these systems use protocols such as SNMP for monitoring network devices on the access layer. Detecting and preventing malicious activities such as unauthorized IP address changes in network monitoring solutions is fast becoming of paramount importance. Network monitoring working in synergy with physical layer security also finds favor, especially in IoT networks; this endeavor strives to provide security enhancement through the exploitation of the physical communication channel properties. In general, the future of network monitoring is one where more intelligent, context-aware, and layered security techniques are employed to counterbalance the evolution of threats.

4) AI Operations

Artificial Intelligence and Machine Learning-based integration is a fine example of how network operations are being reshaped to make infrastructure more autonomous, efficient, and secure. AI-powered systems allow for zero-touch provisioning and self-configuration and self-healing; thereby minimizing the operational burden of managing complex network environments. Another form of good forewarning is troubleshooting, whereby the AI algorithms analyze network data so that potential issues can be predicted and solved before a significant disruption is

brought about. Cisco Catalyst Center and Juniper Mist AI are examples of AIS working towards network automation and anomaly detection. The other key trend is AI-based anomaly detection and security enhancement. AI complements security tools for behavioral analytics, automated threat mitigation, and edge security to present an increasingly adaptive and hardened barrier against unseen cyber threats. AI algorithms analyze traffic patterns, predict congestion, and make dynamic decisions on routing and resource allocation so that networks may be made faster with minimum latency and maximum bandwidth utilization. Intelligent resource allocation means energy efficient operations and highly demanded high performance network services. The concept of Network Digital Twins, virtual replicas of physical networks powered by AI, is gaining momentum as a strategic planning and performance enhancement tool. The digital twins can be used for testing scenarios, predictive maintenance, and designing an optimized network so real decisions may be taken without risk. Interesting, in the final analysis, is the AI/network technology synergy with emerging network technologies such as 5G. AI and ML are fast becoming a mover from supplementing network operations to its core. The trends point to a future where networks become intelligent, self-managing, and proactively maintain performance, security, and efficiency [6], [8], [9].

IV. Using AI assistants to test the ability to create switch configuration and analyze CLI output

We are discussing the usage of modern AI assistants, including ChatGPT, Standard Copilot, Google Gemini, Grok, DeepSeek, in the network engineering domain. We investigate their potential in the creation of switch configurations and in the efficient analysis of CLI output. By testing these AI models, the aim is to provide a discourse on whether these models can adopt and augment important network tasks, that is, to shed some light on whether they can understand logic of network configuration.

1) ChatGPT

An all-purpose large language model developed by OpenAI, ChatGPT aims to generate human like text for varying purposes: content writing, engaging with people, and coding assistance. Its greatest advantages came from its vast knowledge base and strong conversational skills and text generation, making it useful in both everyday and professional problems.

2) Standard Copilot

Standard Copilot tries to boost user productivity by granting AI-powered assistance within familiar workflows. It can assist with anything from summarizing documents to drafting emails, putting forward ideas, or even suggesting code, acting as a companion in day-to-day computing.

3) Google Gemini

Gemini aims to be a multimodal AI from Google that can understand and respond in all formats, presently consisting of text, images, audio, video, and code. The design enables advanced reasoning and problem solving skills, which can be powered by the entire suite of Google services and applications with very intelligent AI capabilities.

4) Grok

Created by xAI, Grok is an AI model that is linked to the social media platform of X (former Twitter). Their goal is to give the freshest and most unfiltered answers of any kind, sometimes conversational and often with wit, distinguishing it from the more formal AI assistants.

5) Deepseek

DeepSeek AI is dedicated to building powerful and efficient language models, with an emphasis on code generation and comprehension. Their models are technically strong when it comes to programming related tasks and provide developers with excellent tools for code completion, bug fixing, and software development workflows.

B. Usage of AI assistants in enterprise networks

The use of AI assistants in enterprise networks represents a promising direction for the semi-automation and of IT processes. We discuss the ability of AI assistants to recognize and diagnose basic Cisco switch show prompts and their ability to advise on troubleshooting. The main idea is that such a model must have a certain representation of human language. To some extent, it models the rules on which our language functions. After reading millions of lines of text, the model creates a representation of realities such as the existence of verbs, nouns, or pronouns and their various functions within a sentence.

As already mentioned, the model acquires this representation by learning to predict the next word based on a given context. It does this by analyzing a large amount of text, from which it tries to deduce which word could logically follow [11].

Considering the versatility and numerous potential uses of language models, we have attempted to explore one such possibility in the realm of enterprise networks. We shall concentrate on the practical verification of their usability in the generation of access switch configurations. We analyze five selected language models and their capability of producing the technically accurate access layer switch configuration. In the next part we shall focus on their ability to diagnose and describe show prompts.

1) Ability to generate basic switch access layer configuration

We have gradually built access layer switch configuration and compared final responses from AI assistants according to the following scale:

1 – flawless configuration
2 – minor errors in the configuration
3 – major errors in the configuration, missing code block
4 – further querying required
5 – unusable configuration

To preserve integrity, we have asked all five AI assistants the same questions. As a separated task, we have decided to also ask AI assistants all previous questions in one prompt in a new chat and compare the outcomes. The assumption is that AI assistants with strong ability to reach chat history can create a better outcome when tasked questions separately. On the other hand AI assistants without strong ability to reach the chat history might do better when tasked all questions in one query.

The output have shown that Copilot and Gemini have been able to create a complex configuration with only minor mistakes that did not cause any major issues. Both AI assistants have shown great promise in creating Cisco access switch configurations that are usable in enterprise networks. ChatGPT on the other hand provided flawless configuration,

but did not follow the instructions that he had been tasked to do. This fact means that the configuration provided by ChatGPT did not meet the requirements that we have requested, and thus further querying have been required. This behavior is interesting especially because in previous test with similar focus on providing Cisco configuration ChatGPT have proved itself as the AI assistant that have provided the most reliable and almost flawless configuration. The same conclusion as with ChatGPT could be applied to DeepSeek, which provided a flawless configuration, but did not meet the criteria that we have requested. The last AI assistant that we asked the configuration questions was Grok. This AI assistant did not provide any usable configuration and thus we were not able to compare it with other AI assistants.

From the previous test that we conducted three months ago we have also concluded that Copilot have created an unusable outcome and was not fit for generating Cisco configuration. This has changed within the timespan of three months as now we can confirm that the configuration provided by Copilot is significantly better than the one provided three months ago. This result further shows continuous improvement and changes in AI assistants. We asked AI assistants the same questions as in the previous test, but instead of asking each question separately we asked them all questions in one query. Copilot and Gemini have shown poorer results than when they were asked questions separately. ChatGPT has shown slight improvement compared to the original questioning. DeepSeek have shown major improvement when we asked it all questions in one query. Grok did not create any configuration and only shortly described used technologies.

2) Ability to diagnose show statements

We will evaluate each AI response based on the following options:

1 – AI assistant described the prompt without any known mistakes

2 – AI assistant described the prompt with minor mistakes

3 – AI assistant described the prompt with major mistakes

Each AI assistant would then be tasked with the same questions. We would then count responses based on criteria and we would give the AI assistant the final evaluation mark between 1 and 3. All show outputs were generated from the Cisco switch that is deployed in a production network. We are also considering the depth of the response provided by each AI assistant.

Q.	Show output validation				
	ChatGPT	***Gemini***	***Copilot***	***Grok***	***DeepSeek***
1	1	2	1	1	2
2	2	1	1	1	2
3	1	1	2	1	1
4	1	1	1	1	2
5	1	1	2	1	2
6	1	3	3	3	3
7	2	1	2	1	1
8	1	1	2	1	1
9	1	2	1	2	2
10	1	1	2	1	1
S.	1.2	1.4	1.7	1.3	1.7

ChatGPT have proven to be the most reliable and correct in analyzing show prompts. Even though Grok was not able to create comprehensive Cisco switch configuration it was able to understand show prompts, analyze and describe them. Copilot and DeepSeek ranked as last.

We propose an idea of using analyzed CLI outputs from AI assistants as a helping tool for network administrators to troubleshoot basic network issues and suggest corrective measures that could semi-automate the process of troubleshooting network problems.

REFERENCES

[1] O. Afolalu and M. S. Tsoeu, "Enterprise Networking Optimization: A Review of Challenges, Solutions, and Technological Interventions," *Future internet,* no. 17, p. 133, 2025.

[2] J. Dobie a R. Holder, „Network System of Systems Manager,“ rev. *Integrated Communications, Navigation and Surveillance Conference*, 2024.

[3] "Campus LAN and Wireless LAN Solution Design Guide," 04 05 2020. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html. [Accessed 2025 05 21].

[4] "Secure Guest Access for Cisco IOS-XE SD-WAN Devices Deployment Guide," 19 05 2020. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-secure-guest-access-deploy-guide.html. [Accessed 2025 05 22].

[5] „Cisco Secure Access Service Edge (SASE) and Security Service Edge (SSE) Architecture Guide,“ 23 01 2025. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/sase-sse-ag.html. [Cit. 23 05 2025].

[6] A. León, D. Perdices, J. L. García-Dorado, J. Ramos a J. Aracil, „An expert-aware Markovian system for end-user proactive troubleshooting in the Network and Security Operations Center,“ *Expert Systems With Applications,* %1. vyd.276, 2025.

[7] L. Yuexi, "Construction of network access Layer security protection System based on zero trust architecture," in *The 4th International Conference on Machine Learning and Big Data Analytics for IoT Security and Privacy*, 2024).

[8] S. Ahmad, A. Haque, H. A. M. Abdeljaber, A. E. Eljialy, J. Nazeer a B. K. Mishra, „Machine Learning Approaches in Cybersecurity to Enhance Security in Future Network Technologies,“ *SN Computer Science,* %1. vyd.6, 2025.

[9] F. Wilhelmi, D. Salami, G. Fontanesi, L. Galati-Giordano and M. Kasslin, "AI/ML-based Load Prediction in IEEE 802.11 Enterprise Networks," in *International Conference on Machine Learning for Communication and Networking*, 2024.

[10] "Cisco Cloud Campus LAN Design Guide (CVD)," 27 08 2024. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-campus/cloud-campus-lan-design-guide.html. [Accessed 2025 05 23].

[11] D. Drost, "A brief history of language models," 12 3 2023. [Online]. Available: https://medium.com/data-science/a-brief-history-of-language-models-d9e4620e025b.